



< **Lie to me** />

“伏特台风 II”

—— 揭密美国政府机构针对美国国会和纳税人的虚假信息行动

〔内容摘要：中国涉“伏特台风”调查报告发布后，在美国政府机构的授意下，美国主流媒体集体噤声，严控评论，调动国家机器极力回避和掩盖证据，进一步暴露了美相关机构肆意编造所谓“伏特台风”组织入侵事件骗取国会财政拨款的事实。为回应国际社会和相关行业研究机构的关切，我们结合已有材料全面披露美国炮制“伏特台风”计划的具体真相，即“伏特台风”计划是由美国政府机构策划实施的一次针对美国国会和纳税人的合谋欺诈行动，其目的是要制造假想敌，以保住美国维持其网络霸权地位的重要法律武器“美国《涉外情报监视法案》（FISA）702 条款”，并利用该条款授予的“无证监视权”持续强化对全球网络空间的“全面掌控”能力，打压排除不愿配合美情报机构实施网络监控的国外竞争对手，维护美国的网络霸权和长期利益。〕

一、引言

2024 年 4 月 15 日，中国国家计算机病毒应急处理中心、计算机病毒防治技术国家工程实验室和 360 数字安全集团联合发布了题为《伏特台风——美国情报机构针对美国国会和纳税人的合谋欺诈行动》的专题报告¹，对美方 2023 年以来集中炒作所谓“伏特台风”组织的真实来源进行了溯源分析，揭示了该组织勒索病毒犯罪团伙的真实面目和美方借此对华炒作的幕后真相：美国情报机构官员、反华政客操纵网络

¹ <https://www.cverc.org.cn/head/zhaiyao/news20240415-FTTF.htm>

安全企业企图通过移花接木、混淆视听的方式，夸大外部网络威胁，欺骗缺乏网络安全知识的美国国会议员和纳税人为其庞大的虚假预算“买单”。报告公开发布后，多家知名媒体向美国驻华大使馆和微软公司驻华分支机构多次进行询问，均未获得正面回应。按照近年来的“惯例”，美国“环球媒体署”（USAGM）授意那些受美国资本控制的国际主流媒体携手对报告进行了“封杀”。

2024 年 4 月 18 日，美国联邦调查局局长克里斯托弗·雷在美国田纳西州范德比尔特大学公开发表讲话，声称由中国政府支持的“伏特台风”组织已经成功入侵了包括 23 个管道运输行业运营商在内的众多美国公司，影响范围遍及通信、能源、水处理等关键基础设施行业。即便是这样一个连正式发布会都算不上的“讲话”，也在美国式的新闻管制制度控制下开展了一波铺天盖地的宣传攻势。我们再次对“伏特台风”行动进行深入思考，并结合最新调查结果对该对华抹黑行动进行全场景还原，发现：美国炮制“伏特台风”计划的起始时间不晚于 2023 年初，是由美国国家安全局（NSA）、联邦调查局（FBI）等美国情报机构幕后策划，美国国会反华议员、司法部、国防部、能源部、国土安全部等多个联邦政府行政单位以及“五眼联盟”国家网络安全主管部门共同参与的一场虚假信息 and 舆论操控行动，符合美式网络营销的典型特征，属于彻头彻尾的、基于精准广告投放的“认知域”

作战。在此次行动中，美国情报机构滥用自身行政权力，操纵网络安全企业和其他行政机构，通过制作传播虚假信息，制造和渲染“中国网络威胁论”，欺骗美国纳税人、国会议员，侵害中国企业合法权益，力推被称为“无证监视法案”的美国《涉外情报监视法案》（FISA）702条款获批延续，并争取国会批准更大规模的预算投入，进一步巩固和强化美国情报机构的网络渗透能力，特别是加强对外攻击和威慑竞争对手和对内监视和控制民众的能力。

“伏特台风”是美国“纸牌屋”政治游戏的又一现实案例。虽然该行动的主要目标是美国国会和普通民众，但通过持续嫁祸中国，也满足了美国垄断资本势力和反华政客妄图在国际政治经济上孤立中国，阻挠遏制中国发展，侵害和瓜分中国企业合法利益的狼子野心，对中国国家安全和核心利益构成威胁和挑战。本文将在上一篇报告的基础上，进一步阐释美国情报机构编造虚假信息的重要证据，并对美国情报机构的邪恶计划和行动过程进行细致还原，向全球民众揭露美国政府机构通过虚假叙事对外转移其国内矛盾，搞乱国际秩序后再下场充当“国际警察”收割他国利益的丑恶面目。

二、美方“自相矛盾”并掩盖证据

为达成其不可告人的目的，美国情报机构策划了本次虚假信息 and 舆论操控活动，但由于牵涉面过大，难免出现疏漏和基层抵触情绪，从而给我们的调查工作提供了突破口和机

会。我方发布报告后，美方为了掩盖证据，竟然指使美国威胁盟（ThreatMon）公司将已经发布的报告内容进行篡改，上演了现实版的“掩耳盗铃”。以下在上一篇报告的基础上，进一步列举和分析美方机构发布的报告、美政府行政部门采取的行动和美国重要政治人物的言论中存在的重大疑点，揭露美方所谓证据和相关言论的自相矛盾。

（一）“暗黑力量”与美方声称“伏特台风”组织的关联更加清晰

上一篇报告中通过谷歌公司 VirusTotal(以下简称“VT”)平台对微软公司²和“五眼联盟”预警通报³中列举的所谓“伏特台风”组织感染指标（IoCs）进行了验证分析，发现该组织与美国威胁盟公司披露的名为“暗黑力量”的勒索病毒犯罪团伙关系密切。报告中直接引用了威胁盟公司报告的内容⁴，并对暗藏在封底图片背后的关联 IP 地址信息进行了披露。美方不仅没有对隐藏相关 IP 地址的行为做出解释，反而指使威胁盟公司公然更改报告内容，使整份报告的篇幅变成了 20 页，虽然其中 17 页仍然属于封底的一部分，但图片后面原附的关联 IP 地址已经不见踪影，同时还忽略了对报告目录进行修改。修改前和修改后的报告如图 1 至图 4 所示。

² <https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/>

³ https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF

⁴ <https://threatmon.io/storage/the-rise-of-dark-power-a-close-look-at-the-group-and-their-ransomware.pdf>

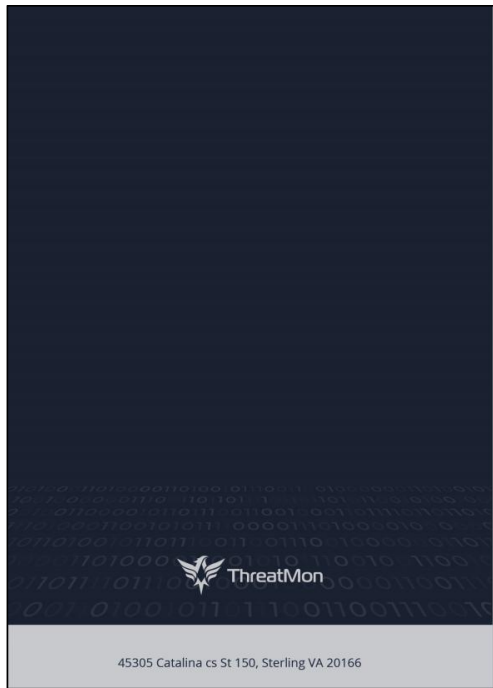


图 1 原威胁盟报告封底

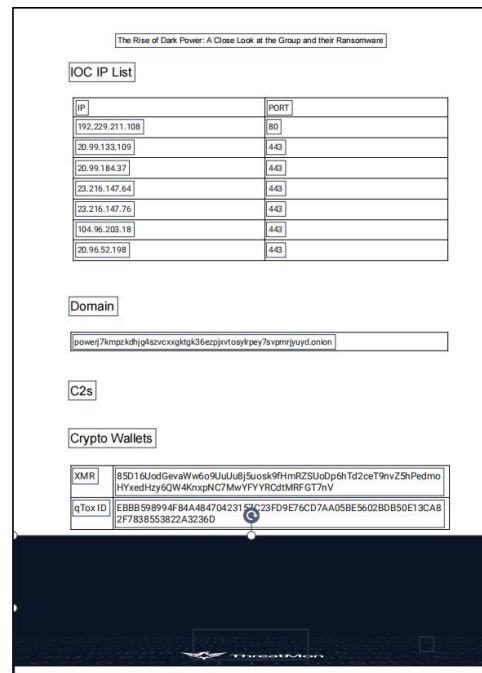


图 2 移动封底图片后威胁盟报告

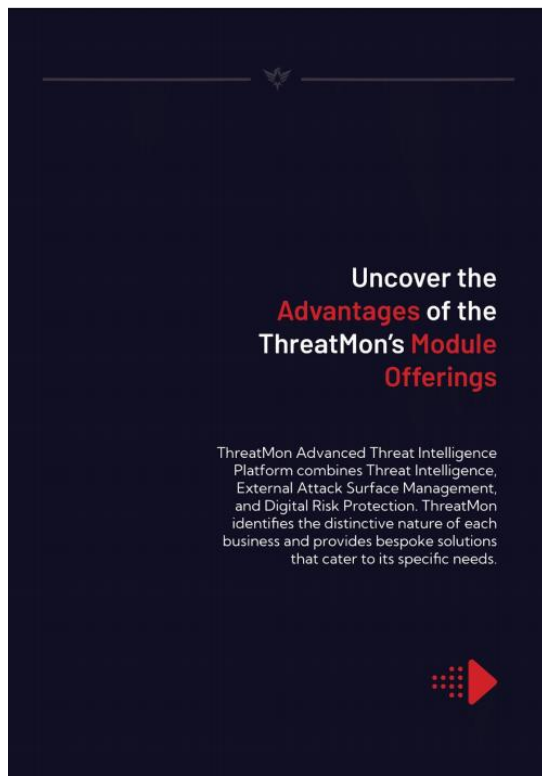


图 3 当前威胁盟报告封底

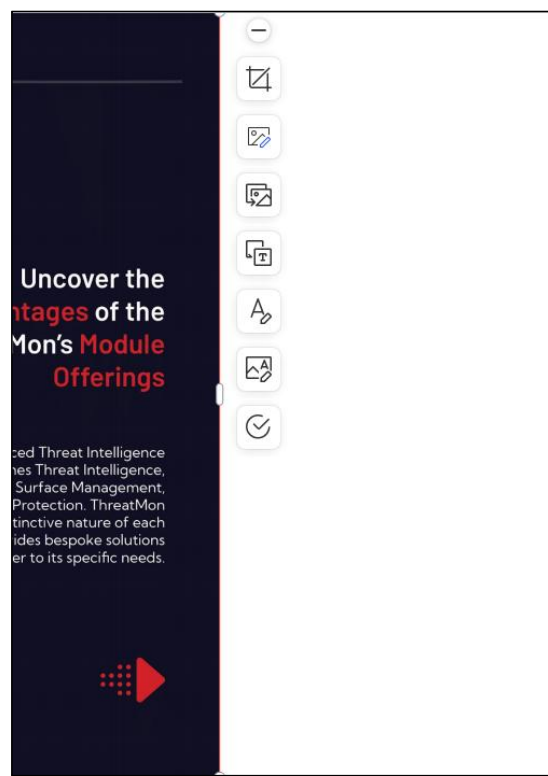


图 4 移动（向左）封底图片后的当前威胁盟报告

我们将在本文附件中提供美国威胁盟公司报告的原始版本和修改后的版本，便于读者进行对比。

美方一定是由于急火攻心、黔驴技穷才出此“掩耳盗铃”

般的下策。但事实就是事实，任何掩盖都是苍白无力的。进一步跟踪调查发现，由美国著名网络安全企业迈克菲公司和火眼公司联合组成的新公司 Trellix 于 2023 年 3 月 23 日发布一篇题为《新勒索病毒团伙“暗黑力量”闪亮登场》（Shining Light on Dark Power: Yet Another Ransomware Gang）⁵的分析报告，对“暗黑力量”组织使用的勒索病毒程序进行了详细技术分析，并且在对“暗黑力量”组织的描述和判断上与威胁盟公司的报告内容完全一致。这份报告中也提供了勒索病毒程序的感染指标，包括两个程序样本的 HASH，如表 1 所示。

表 1 “暗黑力量”相关恶意程序样本

序号	HASH
1	33c5b4c9a6c24729bb10165e34ae1cd2315cfce5763e65167bd58a57fde9a389
2	11ddebd9b22a3a21be11908feda0ea1e1aa97bc67b2dfefe766fcea467367394

值得注意的是，相关程序样本 HASH 与威胁盟公司报告中提供的样本 HASH 也完全相同。如图 5、图 6 所示。

DarkPower Ransomware And Groups IOC's	
IOCs	
TYPE	VALUE
SHA256	33c5b4c9a6c24729bb10165e34ae1cd2315cfce5763e65167bd58a57fde9a389 11ddebd9b22a3a21be11908feda0ea1e1aa97bc67b2dfefe766fcea467367394
SHA1	9bddcce91756469051f2385ef36ba8171d99686d
MD5	df134a54ae5dca7963e49d97dd104660

16

图 5 威胁盟报告中的样本 HASH

⁵ <https://www.trellix.com/blogs/research/shining-light-on-dark-power/>

Appendix C - IoCs

SHA256 hashes of the analysed samples:

```
33c5b4c9a6c24729bb10165e34ae1cd2315cfe5763e65167bd58a57fde9a389  
11ddebd9b22a3a21be11908feda0ea1e1aa97bc67b2dfefe766fcea467367394
```

This document and the information contained herein describes computer security research for educational purposes only and the convenience of Trellix customers. Any attempt to recreate part or all of the activities described is solely at the user's risk, and neither Trellix nor its affiliates will bear any responsibility or liability.

图 6 Trellix 报告中的样本 HASH

继续使用谷歌公司的 VT 平台⁶对相关程序样本 HASH 进行查询，发现这些样本关联的 IP 地址与中方前述报告中列举的 5 个关键 IP 地址完全重合。如图 7、图 8 所示。该分析过程具有高度可重复性，世界各地的网络安全人员都可以利用 VT 平台验证和复现上述结论。问题出现了，谷歌公司会不会迫于美国政府机构的压力，从此禁止来自于中国的用户访问或使用 VT 平台？

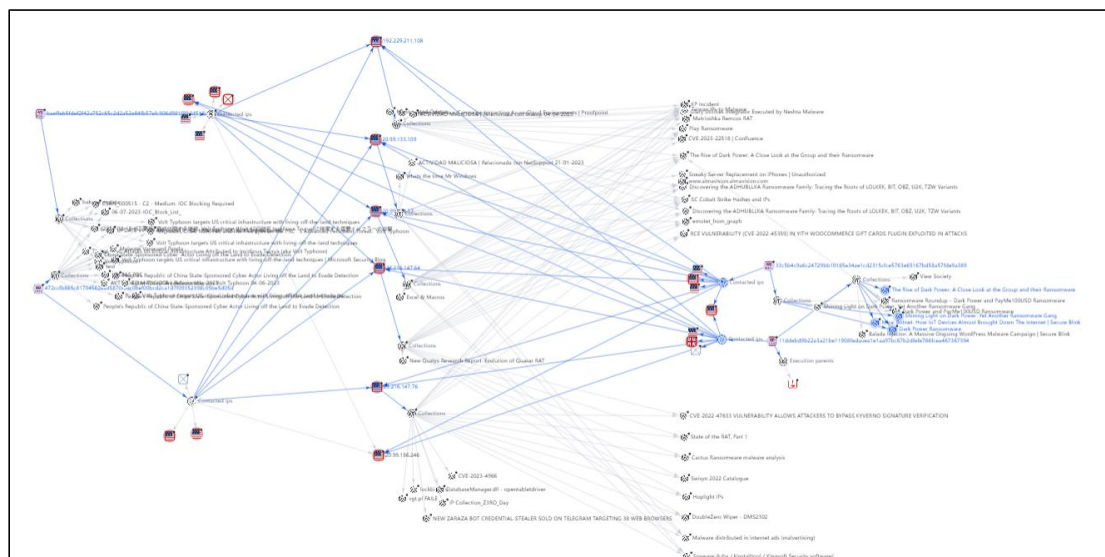


图 7 暗黑力量样本 HASH 与“伏特台风”组织样本的 IP 地址关联关系

⁶ <https://www.virustotal.com/gui/graph-overview>

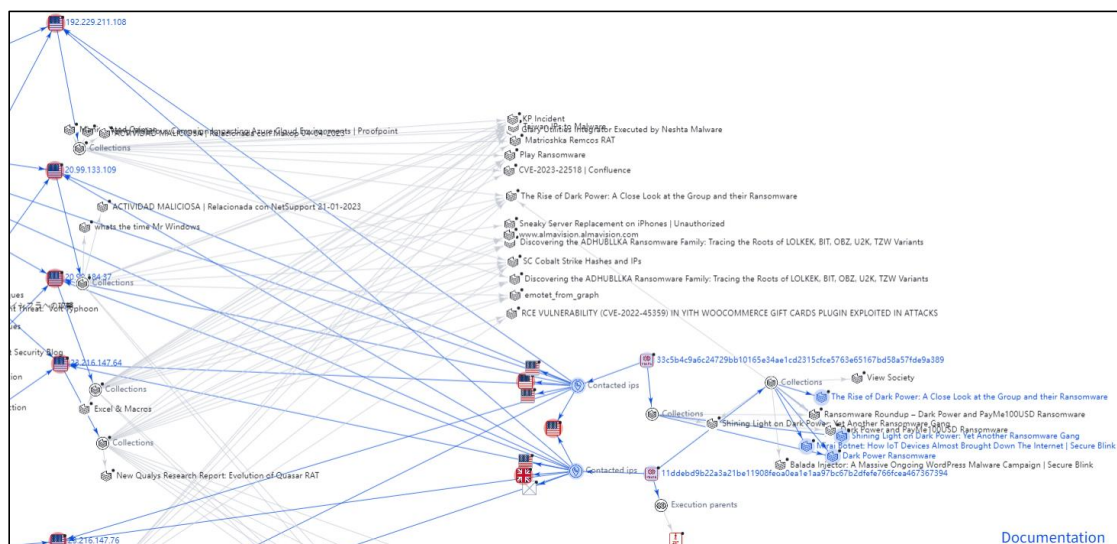


图 8 暗黑力量样本 HASH 与“伏特台风”组织样本的 IP 地址关联关系（续）

实际上，据威胁盟公司不具名人士提供的消息称，威胁盟公司是受到了美国政府相关部门的施压后，对报告进行了修改。由此我们可以推断，美国的网络安全企业广泛存在被美国情报机构操纵的情况。只是威胁盟公司的技术人员采用了更加“艺术”的表现形式，用封底“黑幕”掩盖 IP 地址列表。同时也解释了微软公司的报告中为什么会出现如此低水平的感染指标数据。

（二）美国官方口径与网络安全企业存在明显出入

“五眼联盟”国家的预警通报和微软公司报告中都声称，“伏特台风”组织入侵了美国网件（Netgear）公司等供应商生产的网络设备，并将其作为跳板（进一步实施攻击）。实际情况是，2023 年 5 月 26 日（微软公司报告发布后 2 天），美国网件公司发布了针对“伏特台风”组织攻击的安全公告⁷，在公告中公开表示尚未发现所谓“伏特台风”组织针对该

⁷ <https://kb.netgear.com/000065688/Security-Advisory-Regarding-Volt-Typhoon>

公司产品的任何漏洞攻击活动，这与“五眼联盟”国家炮制的预警通报和微软公司臆测的报告内容明显出入。如图 9 所示。

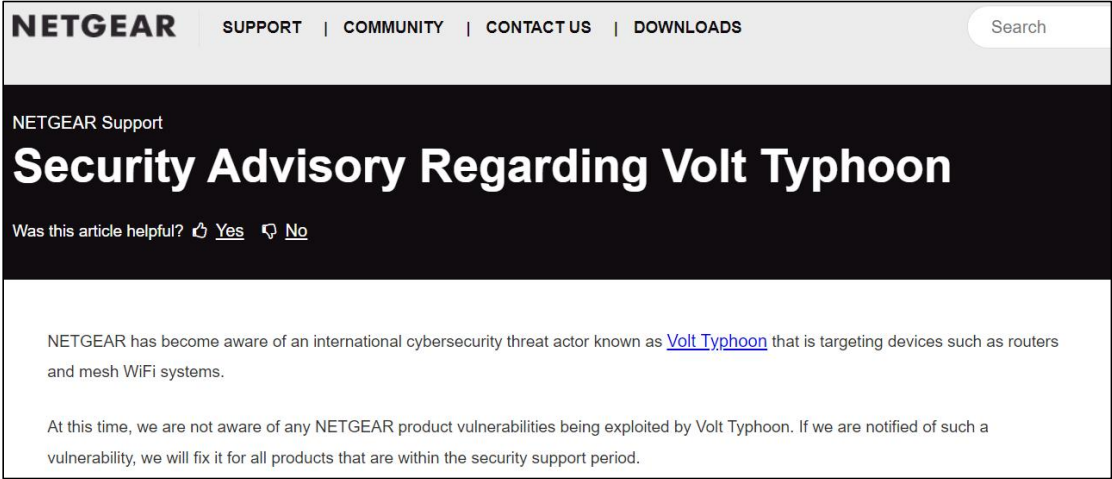


图 9 美国网件公司安全公告

2024 年 2 月 7 日，美国国土安全部下属美国网络安全与基础设施安全局（CISA）发布了一则名为《中华人民共和国支持的黑客组织持续入侵控制美国关键基础设施》（PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure）的安全公告⁸，声称“伏特台风”组织已经入侵了美国本土和海外领地的多个关键基础设施网络，涉及交通、能源、运输、供水和水处理等多个行业，并刻意在上述“五眼联盟”预警通报和微软公司报告所含技术细节的基础上增加了一些内容，宣称，“伏特台风”组织利用了英万齐（Ivanti）公司 VPN 产品的 Connect Secure 漏洞实施了入侵。然而公开打脸的事情再次发生，2024 年 4 月 5 日，美国谷歌公司旗下著名的网络安全威胁情报公司曼

⁸ <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>

迪安特 (Mandiant) 发布了一篇题为《前沿 4: 英万齐 Connect SecureVPN 产品漏洞利用后渗透和横向移动案例研究》⁹ (Cutting Edge, Part 4:Ivanti Connect Secure VPN Post Exploitation Lateral Movement Case Studies)。曼迪安特公司报告中指出,2024 年 2 月,该公司发现并跟踪了一个尚未被分类的黑客组织“UNC5291”,认为该组织与“伏特台风”的同源性只能达到中等概率程度。同时还明确表示,该公司至今尚未发现“伏特台风”组织成功入侵了英万齐公司的 Connect Secure 产品。曼迪安特公司的表述如图 10 所示。

In February 2024, Mandiant identified a cluster of activity tracked as UNC5291, which we assess with medium confidence to be Volt Typhoon, targeting U.S. energy and defense sectors. The UNC5291 campaign targeted Citrix Netscaler ADC in December 2023 and probed Ivanti Connect Secure appliances in mid-January 2024, however Mandiant has not directly observed Volt Typhoon successfully compromise Ivanti Connect Secure.

图 10 美国曼迪安特公司报告节选

从以上案例中我们不难看出,“五眼联盟”国家预警通报和微软公司报告并未得到美国国内其他网络安全企业的一致认同,而且参与“调查”的美国网络安全主管部门也明显没有向相关企业分享具体的攻击案例和技术细节。

(三) 美国网络安全主管部门行为前后矛盾

⁹ <https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement>

我们发布的上一篇报告中提到，2024 年 1 月 31 日，美国司法部网站公开发布题为《美国政府破坏了中华人民共和国用来掩盖针对美国关键基础设施实施网络攻击的僵尸网络》的通报¹⁰，称 2023 年 12 月，经法院授权，美国司法部开展专项行动，从美国全国数百台路由器上成功清除了 KV 僵尸网络程序。美国司法部长梅里克·加兰、美国联邦调查局局长克里斯托弗·雷和美国司法部国家安全司助理司法部长马修·G·奥尔森等高官在相关事件信息发布会上一致表示美国司法部的此次行动破坏了所谓的“中国国家支持的黑客”入侵美国关键基础设施的努力。然而，2024 年 4 月 18 日，美国联邦调查局局长克里斯托弗·雷在美国田纳西州范德比尔特大学公开讲话¹¹时却声称“与中国政府有关的黑客组织已经潜入美国关键基础设施，并正在等待适当的时机实施毁灭性打击”。既然美国政府机构在 2024 年初就已经宣布成功挫败了所谓的“中国网络攻击”，为何时隔 2 个多月后却全面否定了自己已经取得的“突出”工作成绩？难道美国高官们的记忆仅仅保持不足 2 个月？

在如此疑点重重、模糊不清的情况下，美国网络安全主管部门仍然坚持杜撰了一个看似丰满其实却是千疮百孔的所谓“国家支持背景的”黑客组织。事实上，这样的归因根

¹⁰ <https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical>

¹¹ <https://www.reuters.com/technology/cybersecurity/fbi-says-chinese-hackers-preparing-attack-us-infrastructure-2024-04-18/>

本无法令人信服，暂且将美国杜撰这种缺乏明显差异性特征且归因模糊的黑客组织称之为“口袋”组织，也就是很难分清楚，装“谁”都可以。作为号称全球网络空间第一强国的美国偏偏要费尽心机地杜撰一个这样的“口袋”组织，其反常行为和众多疑点都让人不得不怀疑，事件的幕后操纵者一定有着不惜一切代价也要达到的目的。而当2024年4月20日美国总统拜登签署了一份由美国国会审议通过的法案后，一切就都明朗起来了。

三、“伏特台风”行动复盘

在上一篇报告中，我们揭露了美方编造“伏特台风”谎言的真实意图，即：具有浓厚政府背景的美网络安全机构在向美国国会申请预算的关键时间节点发布相关虚假信息，旨在配合美国情报机构申请预算拨款，微软等网络企业也可借此获得美政府的大额合同。然而，众所周知，**美国金钱政治的本质就是“钱权交易”**，争取预算经费固然重要，但争取预算的依据来自其现有职能，这些机构的职能表面上仍然依赖于法律授权，因此，法律授予的权力同样是美国情报机构的“命根子”。

2023年伊始，作为美国情报界当之无愧的“带头大哥”，时任美国国家安全局局长兼美国网络司令部司令中曾根就忧心忡忡地表示，其当时最为担心的两件事情正朝着不利的方向发展。

第一件事情涉及美情报机构对全球的所有国家和地区施加无差别迫害。美国情报机构在全球和美国国内实施互联网监控的重要法律依据《涉外情报监视法案》¹²（Foreign Intelligence Surveillance Act, FISA）第 702 条款（以下简称“702 条款”）即将于 2023 年底到期作废。《涉外情报监视法案》颁布于 1978 年，是美国情报机构开展对外情报收集所必须遵循的重要法理依据和法律框架。法案中的“702 条款”¹³在该法案 2008 年修订时被加入其中，该条款授权美国政府机构对身居美国境外的外国人有针对性地实施情报监视，并强迫谷歌、微软、苹果、脸书等互联网科技公司交出公司运营中采集到的全部非美国公民个人数据。爱德华·斯诺登在 2013 年披露的美国国家安全局（NSA）臭名昭著的互联网监控项目“棱镜计划”就是在该法律条款授权下进行的，由此可见“702 条款”对于美国情报机构的重要性。

由于被美国各大情报机构持续滥用，“702 条款”在美国国内和全球各国一直饱受争议，然而美国情报机构却一直以所谓反恐工作需要为由，推动该条款的反复延续。在此背景下，该条款于 2018 年再次获批延续，延续时间截至 2023 年底。由于众所周知的原因，自 2018 年以来，美国面临的国际国内形势发生了重大变化，恐怖活动已不再是美国的最大威胁，美国国家安全战略中已经公然将中、俄、朝、伊列为

¹² <https://crsreports.congress.gov/product/pdf/IF/IF11451>

¹³ <https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf>

主要战略竞争对手。新冠病毒肺炎疫情期间，美国国内爆发“黑命贵”运动，美国总统大选结果引发争议导致占领国会山的“风景线”运动，美国情报机构面临的挑战和承受的压力越来越大，特别是在其国内政治斗争中屡屡被推上“风口浪尖”。美国情报总监办公室的公开报告表明，美国情报机构每年滥用“702 条款”针对美国公民实施的监控行动超过 20 万次¹⁴。美国前总统特朗普及其支持者也反复抨击美国情报机构滥用“702 条款”，以特殊手段动态掌握其竞选活动的动向，暗助民主党和拜登政府打压竞选对手；与此同时，美国国内大量民权机构持续呼吁废止“702 条款”，导致该条款的延续面临严峻挑战。一旦“702 条款”未能获批延续，美国诸多情报机构严重依赖的互联网情报收集手段将失去法律依据，各大情报机构将不得不在表面上暂停网络和电信监控活动，美国情报机构赖以生存的全球范围监听、监视能力将遭到严重削弱，与此相应的大量情报监控系统 and 网络武器系统将被迫在表面上暂时停用（事实上从未停止过），“**五眼联盟**”将变成“**近视眼**”联盟，其通过打压和禁用华为产品而勉强维持的通讯和网络监控能力将再次受到冲击。这也意味着大量美国财政预算被削减，美国网络科技企业、网络安全企业、军工企业将失去大量订单，高度依赖政府订单而生存的美国网络安全行业将集体遭遇重大挫折，那些向该行

¹⁴ https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf#page=24

业投入巨资的豪门望族在美国政府机构中的代理人也由此陷入深度焦虑。

另一件事情与迫害中国企业有关，中国互联网企业的产品和服务在全世界流行程度持续提高，但这些互联网企业长期游离于美国情报机构的掌控范围之外，从概念上严重威胁美国的“国家安全”。即使“702 条款”再次得以延续，由于其不可避免的中国母公司背景，美国情报机构无法像控制谷歌、微软、Meta、苹果等美国互联网企业一样对中国互联网企业为所欲为。这对于美国情报机构来说简直是不可容忍的重大隐患，必须早做打算。

2023 年 1 月 12 日，时任美国国家安全局局长兼网络司令部司令中曾根公开敦促¹⁵美国国会继续延续“702 条款”并授予情报机构更加广泛的监视权力。中曾根宣称，“702 条款”在帮助情报机构抵御勒索病毒攻击、防止武器非法扩散，以及用于识别对美军现实威胁方面发挥了“不可替代”的作用。此次讲话重点围绕所谓“网络安全”话题展开，中曾根自己也很清楚，当今时代继续渲染反恐需要已很难站得住脚，难以与被忽悠方产生共情，权宜之计，只能从渲染外部网络攻击威胁入手继续实施“社工”行动（即：社会工程学攻击，一种利用受害人心理弱点实施的以欺诈为主的恶意活动）。

然而，光凭电诈话术当然无法赢得美国会议员们的信服，

¹⁵ <https://therecord.media/nakasone-foreign-surveillance-program-helped-fend-off-cyber-attacks>

必须要拿出实打实的“工作业绩”。在此背景下，美国情报机构必须团结起来维护自身核心利益，迫切需要找到一个“一石二鸟”的计划来应对上述两个燃眉之急。鉴于相关计划主要围绕所谓“伏特台风”组织展开，不妨将其命名为“伏特台风计划”。现有情况和数据显示，“伏特台风”计划至少起始于2023年初，很可能更早。策划组织实施这样一个涉及多部门、多国家和众多私营企业的计划必定需要花费大量时间，根据后续该计划的实际执行情况，我们可以将其大致划分为三个阶段。

（一）准备阶段（2023年1月至2023年5月）

该阶段的主要任务是找到一个其他国家（主要包括中国、俄罗斯、朝鲜和伊朗）针对美国的网络攻击的案例。为了便于后续“社工”行动的顺利实施，攻击者最好是“中国政府支持”的黑客组织，而受害者的严重程度则越高越好，最起码也得是美国境内或其海外军事基地的“关键基础设施”；为便于初期操作，受害单位最好是位于一个地处偏远且能够被美国情报界绝对控制的地区。按照这个思路，我们不难判断，“关岛”简直就是一个完美的“受害者”。作为美国重要的海外领地，关岛拥有美国在西太平洋地区最大的海空军基地，战略位置极其重要，并且该基地的主要职责定位就是威慑中国，只要公开声称中国对关岛的美国军事设施和通信设施实施了网络攻击，该计划就立即成功了一大半。美军在

关岛及其周边地区层层部署的网络安全监测防护系统，都可以在特定情况下暂时“失效”，让岛上的关键基础设施“真正”遭受某种攻击。至于网络攻击实施者，只要能找到一个完美的“替罪羊”，也就是前面提到的“口袋”组织就足够了，技术报告写得越详细越好，归因溯源理由根本不重要。

下一个问题就是找一个“出头鸟”，把这件事情捅出去，这时，微软公司主动站了出来。微软公司在当时可谓郁闷至极，本来在 2019 年成功击败亚马逊公司拿到美国国防部总价值 100 亿美元的云计算项目“联合企业防御基础设施”（Joint Enterprise Defense Infrastructure，JEDI），却在拜登政府上台后，于 2021 年 7 月被美国国防部撤销¹⁶。随后，2022 年 12 月 7 日，美国国防部宣布启动“联合战争云项目”（Joint Warfighting Cloud Capability，JWCC），项目总预算变成 90 亿美元，并且由亚马逊、甲骨文、谷歌和微软 4 家公司共同承建并展开竞争。眼看着独享的“太平层”变成了“四人间宿舍”，微软显然非常不甘心，急于好好表现，尽可能把失去的份额抢回来。而且微软公司也很清楚，JWCC 项目就是为了情报收集和分析，一旦“702 条款”有个三长两短，包括 JWCC 项目在内的一系列大额订单就会彻底泡汤，因此微软公司必须配合美国情报机构把项目预算保住。

为了让整个事件显得更为可信，还必须拉上一些“外来

¹⁶ <https://edition.cnn.com/2021/07/06/tech/defense-department-cancels-jedi-contract-amazon-microsoft/index.html>

和尚”，“五眼联盟”国家的情报机构属于利益共同体，一起出面策应也是顺理成章。

2023年5月8日，中曾根在美国田纳西州纳什维尔范德比尔特大学举办的2023年度“现代冲突和新兴威胁峰会”上¹⁷声称，美国将坚持“防线前移”的进攻性网络防御策略，持续开展“前出狩猎”网络行动，同时还重点提出了对“702条款”即将到期问题的观点，指出如果国会未能在年底前完成重新授权，美国情报界将会面临重大损失。

随后，面对2023年5月19日美国外国情报监视法院公开¹⁸批评美国情报机构在2021年1月6日国会山抗议事件和2020年“黑命贵”抗议活动期间滥用“702条款”的压力。美国情报机构不得不加速“伏特台风”计划。2023年5月24日，经过近半年的密谋，“伏特台风”计划的第一场揭开帷幕，“五眼联盟”国家¹⁹和微软公司²⁰的报告相互呼应，再加上受美国资本和情报机构操控的媒体铺天盖地地宣传，有效转移了公众对美国政府机构滥用“702条款”的关注视线，可谓初战告捷。计划第一阶段取得的良好预期效果，为下一阶段的重点任务奠定了良好基础。

（二）攻坚阶段（2023年6月至2024年1月）

¹⁷ <https://therecord.media/nakasone-cyber-strategy-section-702-hunt-forward-russia-ukraine-nato>

¹⁸ https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf

¹⁹ https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF

²⁰ <https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/>

第二阶段的重点任务有两个，一是确保“702 条款”获得延期，二是争取在 2025 财年增加预算。第一阶段的良好开局，微软公司功不可没，带头示范效应明显，在随后的几个月中，美国谷歌公司²¹、黑莓公司²²、CrowdStrike 公司²³、Dragos 公司²⁴、飞塔公司²⁵等纷纷跟进炒作“伏特台风”，内容五花八门，让人眼花缭乱，“伏特台风”简直成了美国电影中无所不能的超人。这主要归功于美国情报机构和微软公司联合采取的“口袋”组织策略，这种策略给后来者创造了宽广的想象和发挥空间。

距离 2023 年底越来越近了，“702 条款”到期延续问题迫在眉睫。在 2023 年 12 月 5 日美国国会参议院听证会上，联邦调查局（FBI）局长克里斯托弗·雷亲自为“702 条款”辩护²⁶，面对参议员们关于联邦调查局（FBI）滥用该条款的质疑，克里斯托弗·雷反复声称，“702 条款”对打击网络犯罪和恐怖主义活动至关重要。

2023 年 12 月 8 日在美国弗吉尼亚州阿灵顿举行的一次美国情报界和国家安全联盟活动中，中曾根再次站出来公开呼吁美国国会重新授权 702 条款²⁷。由此也拉开了本计划第

²¹ <https://cloud.google.com/blog/topics/threat-intelligence/chinese-espionage-tactics>

²² <https://blogs.blackberry.com/en/2023/08/bb-protects-from-volt-typhoon>

²³ <https://www.crowdstrike.com/blog/falcon-complete-thwarts-vanguard-panda-tradecraft/>

²⁴ <https://hub.dragos.com/report/voltzite-espionage-operations-targeting-u.s.-critical-systems>

²⁵ <https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign>

²⁶ <https://www.usatoday.com/story/news/politics/2023/12/05/fbi-director-christopher-wray-702-surveillance-senate-judiciary/71813997007/>

²⁷ <https://www.c4isrnet.com/battlefield-tech/it-networks/2023/12/08/cyber-commands-nakasone-urges-renewal-of-foreign-spy-law/>

二阶段的冲刺进程。

果然，在 2023 年 12 月 13 日，美国国防部的另一个御用供应商，美国流明科技（Lumen Technologies, Inc）公司跳了出来，发布报告²⁸再次炒作“伏特台风”组织，并认为该组织在网络攻击活动中利用被命名为“KV 僵尸网络”（KV-Botnet）的物联网僵尸网络作为跳板。在美国环球媒体署（USAGM）的授意下，该报告再次引发媒体热议并掀起新一轮“中国威胁论”炒作。

面对美国国内日益高涨的反对声音，美国情报机构耍了个小聪明，将关于申请“702 条款”延续的法案在最后一刻“夹带”进了必须获得通过的 2024 财年国防授权法案（NDAA）中。尽管美国超过 30 个社会组织联名致信美国国会要求将关于“702 条款”续期的内容撤出国防授权法案（NDAA）²⁹，但该法案还是于 2023 年 12 月 22 日最终获得通过，“702 条款”得以延期至 2024 年 4 月 19 日³⁰。

对于美国情报机构来说，虽然暂时未达成将“702 条款”长期延续的预期，但总算可以缓一口气，但还有一个艰巨任务是争取增加下一财年的预算——必须赶在 2024 年 2 月 5 日总统提交下一财年预算之前，把准备工作做充分。因此，2024 年 1 月 31 日，美国司法部宣称通过组织专项行动，从

²⁸ <https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/>

²⁹ <https://www.brennancenter.org/our-work/research-reports/coalition-letter-urges-congressional-leaders-keep-reauthorization-section>

³⁰ <https://www.congress.gov/118/plaws/publ31/PLAW-118publ31.pdf#page=974>

美国全国数百台路由器上成功清除了 KV 僵尸网络程序³¹。美国网络安全与基础设施安全局(CISA)和联邦调查局(FBI)共同宣称中国政府支持的“伏特台风”组织在内的黑客组织正在针对小型商用和家用网络设备进行攻击³²。而最重要的“汇报演出”也在 2023 年 1 月 31 日上演，美国国会众议院中国问题特别委员会在华盛顿众议院办公楼举行了主题为“中国对美国国土和国家安全的网络威胁”听证会³³。美国国会著名反华议员，时任美国国会中国问题特别委员会主席，麦克·加拉格尔(Mike Gallagher)主持会议，以中曾根为首的美国情报机构主要负责人悉数出席，通过讨伐所谓“中国政府支持的”黑客组织获得国会议员的共鸣，将“伏特台风”计划推向高潮。美国联邦调查局(FBI)局长克里斯托弗·雷更是在听证会上公开宣称³⁴，“702 条款是联邦调查局(FBI)打击中国黑客组织的最强大工具。”充分暴露了此次听证会的真实目的，就是以所谓中国黑客网络攻击威胁为幌子，谋求“702 条款”续期以继续维持美国情报机构对包括中国在内的全球网络用户实施无差别“无证监视”的权力及其相关经费保障。这些成果在美国 2025 财年预算中得到了体现³⁵。

³¹ <https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical>

³² https://www.cisa.gov/resources-tools/resources/secure-design-alert-security-design-improvements-soho-device-manufacturers?utm_source=FBI&utm_medium=press_release&utm_campaign=SbD_SOHO

³³ <http://selectcommitteeontheccp.house.gov/committee-activity/hearings/hearing-notice-ccp-cyber-threat-american-homeland-and-national-security>

³⁴ <https://selectcommitteeontheccp.house.gov/media/press-releases/chairman-gallaghers-opening-remarks-and-witness-testimony-2>

³⁵ https://www.whitehouse.gov/wp-content/uploads/2024/03/budget_fy2025.pdf

至此，“伏特台风”计划的目标初步达成，但却并不完美，因为“702 条款”的授权期限仅仅延长到了 2024 年 4 月 19 日，远未达到预期。

（三）成果巩固阶段（2024 年 2 月-2024 年 4 月）

随着该条款到期日的再次临近，美国国内的反对“702 条款”延续的声音越来越大，美国前总统特朗普也声称其成为“702 条款”直接的受害者³⁶，美国民主斗士斯诺登和代表西方式网络正义的“维基解密”也分别通过 X 平台（前推特平台）不断发声，呼吁美国民众反对“702 条款”的再次续期。

与此同时，美国各情报机构则按照既定计划持续不断地以所谓“伏特台风”组织渲染中国网络安全威胁，并再次利用“五眼联盟”情报协作机制，给“702 条款”续期营造有利的舆论氛围。

正如前文已经提到的那样，2024 年 2 月 7 日，美国国土安全部下属的美国网络安全与基础设施安全局（CISA）伙同能源部、环境保护局等多个美国联邦政府部门，以及其他四个“五眼联盟”国家网络安全主管部门，联合发布了一则名为《中华人民共和国支持的黑客组织持续入侵控制美国关键基础设施》（PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure）的安

³⁶ <https://thehill.com/policy/national-security/4584988-trump-on-warrantless-surveillance-reauthorization-kill-fisa/>

全公告³⁷，再次将“伏特台风”搬出来，试图转移美国国会议员和民众注意力，继续渲染虚假的中国网络攻击威胁。而在2月7日举行的相关记者会上，美国联邦调查局（FBI）网络安全部副主任助理辛西娅·凯泽（Cynthia Kaiser）透露³⁸，FBI调查人员利用“702条款”实施监视并收集的数据发现了所谓来自中国的黑客组织针对美国关键基础设施的攻击活动，但拒绝透露进一步细节。这也进一步证明了，“伏特台风”计划就是美国情报机构为“702条款”续期所准备的重要“筹码”。而且，美国情报机构完全可以以保密为由，拒绝向社会公开溯源调查细节，而美国现任国会议员作为非专业人士，即便看到了所谓的溯源分析证据，也无法做出正确的判断。

2024年3月19日，美国网络安全与基础设施安全局（CISA）又抛出了一份名为《中华人民共和国支持的黑客组织的网络攻击活动：针对关键基础设施主管单位的预警通报》³⁹（PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders），对美国私营关键基础设施运营单位进行“敲打”。由于很多美国的私营关键基础设施运营单位不愿意增加网络安全成本，美国网络安全与基础设施安全局对此一直“耿耿于怀”。而对于美国微软公司等众多美国网

³⁷ <https://www.cisa.gov/news-events/alerts/2024/02/07/cisa-and-partners-release-advisory-prc-sponsored-volt-typhoon-activity-and-supplemental-living-land>

³⁸ https://www.theregister.com/2024/02/09/fbi_volt_typhoon_section_702/

³⁹ <https://www.cisa.gov/resources-tools/resources/prc-state-sponsored-cyber-activity-actions-critical-infrastructure-leaders>

络安全企业来说，美国关键基础设施网络安全建设这块“大蛋糕”势在必得，而且也应该是其参与“伏特台风”计划的“合理回报”。因此美国网络安全与基础设施安全局不惜利用行政权力“恐吓”这些私营单位，逼迫私营单位增加网络安全投入，为美国网络安全企业及其背后的资本家争取更大利益。

2024 年 4 月 9 日，一份名为《改革情报工作和保护美国》的法案（Reforming Intelligence and Securing America Act, RISAA）被提交众议院审议，该法案提出将“702 条款”延期两年，并进一步扩大了“702 条款”中对“电子通信服务提供商”（ECSP）的定义，也意味着“702 条款”能够监视的范围进一步扩大。

2024 年 4 月 12 日，就在美国国会众议院即将审议《改革情报工作和保护美国》法案当天，接替中曾根职务的蒂莫西·豪将军⁴⁰代表美国网络司令部公开发表了 2024 年度“态势声明”⁴¹，再次点名中国、俄罗斯、伊朗和朝鲜的网络攻击活动对美国及其盟友国家安全构成威胁，还特别指出“美国网络司令部将尤其关注并加强防范中国针对美国关键基础设施的攻击。”最终，经过激烈交锋，美国国会众议院以 273 票对 147 票批准该法案并提交参议院审议。

该法案通过众议院审议后，美国民众仍然没有停止呼吁

⁴⁰ <https://defensescoop.com/2024/02/02/timothy-haugh-takes-over-cyber-command-nakasone/>

⁴¹ <https://www.cybercom.mil/Media/News/Article/3739700/posture-statement-of-general-timothy-d-haugh-2024/>

否决该法案的努力。2024 年 4 月 16 日，包括美国电子隐私信息中心（EPIC）在内的 70 余家民间机构联名致信⁴²美国国会参议院议员，请求参议院否决该法案。

2024 年 4 月 18 日，在美国国会参议院对“702 条款”延期法案进行投票的前一天，美国联邦调查局（FBI）局长克里斯托弗·雷在美国田纳西州范德比尔特大学公开发表言论，声称中国政府支持的“伏特台风”组织已经成功入侵了包括 23 个管道运输行业运营商在内的众多美国公司，再次散布虚假消息操控舆论，向参议院施加压力。

最终，在“702 条款”授权的最后期限，2024 年 4 月 19 日，美国国会参议院以 60 票对 34 票通过了该法案，并在 4 月 20 日提交美国总统拜登后迅速获得签署批准。

而与此同时，针对中国互联网企业的打压也在有序推进，在“伏特台风”行动的渲染下，一切与中国有关的网络安全威胁都得到高度重视。

美国总统拜登在 2024 年 2 月 28 日签署了关于限制中国和其他外国战略对手获取美国敏感个人数据的第 14117 号行政命令《防止受关注国家访问美国人的大量敏感个人数据和与美国政府有关的数据》⁴³。该行政令要求司法部长颁布法规，明确保护美国人的敏感个人数据免遭特定国家的大规模转移和滥用，并加强对政府相关敏感数据的保护。

⁴² <https://epic.org/epic-coalition-urge-opposition-to-risaa-terrifying-expansion-of-fisa-section-702/>

⁴³ <https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/>

2024 年 3 月 13 日，美国国会众议院突然以 352 票对 65 票的压倒优势投票表决通过了由时任威斯康星州共和党议员、美国国会中国问题特别委员会主席麦克·加拉格尔提出的 H.R.7521 的法案《保护美国人免受外国战略对手控制的应用程序侵害法案》（Protecting Americans from Foreign Adversary Controlled Applications Act），禁止在美国内对被外国战略对手国家控制，并被美国总统确定为对美国国家安全构成重大威胁的应用程序进行分发、维护或提供互联网托管服务。加拉格尔声称，为防止该法案被提前泄露给媒体，其已经与同事们秘密准备了 8 个月，可谓处心积虑。西方主流媒体分析认为，该法案能够快速顺利通过的主要原因，就是美国民主党议员和共和党议员都认为中国互联网企业对美国国家安全构成了风险，这其中当然也有“伏特台风”计划的功劳。2024 年 4 月 23 日，美国众议院议长约翰逊将上述法案捆绑在一系列总计 950 亿美元的援助乌克兰和以色列的紧急补充拨款法案中，一起通过了参议院投票审议。在参议院投票前，美国参议院“情报”委员会主席、著名反华政客马克·沃纳还专门向参议院发表演说并声称，普通美国民众无法获悉美国情报机构提供的“秘密情报”，因此不了解中国互联网企业产品对“美国国家安全构成的风险”。并鼓吹这些产品“不应该由被美国法律所认定的‘对手’国家所拥有和控制”。而所谓的“秘密情报”必然是“702 条款”

的“成果”，而且“欲加之罪，何患无辞”，这对拥有“无证监视权”的美国情报机构来说完全是驾轻就熟。

2024年4月24日，上述法案由美国总统拜登签字生效。

至此，尽管过程艰难曲折，美国情报机构终于志得意满，迎来了“伏特台风”计划的全面胜利。在未来的两年里，美国情报机构不但保住了手中的权力，获得了更高的预算，扩大了监控范围，还有望将中国互联网企业挤出美国市场。

最后，虽然为“伏特台风”计划的成功立下汗马功劳的前美国国家安全局局长兼网络司令部司令中曾根将军在2024年2月退休，但美国政府机构、情报界和网络安全企业及其背后的资本家们当然懂得“吃水不忘打井人”的道理。2024年6月13日，著名的美国人工智能创新企业，大名鼎鼎的“ChatGPT”的缔造者，OpenAI公司宣布聘请中曾根为该公司董事会成员⁴⁴。众所周知，OpenAI公司的最大股东是微软公司。显然，中曾根将军作为公司高管，在享受高薪的同时也会“帮助”OpenAI公司更好的遵守“702条款”。而且2024年6月10日，OpenAI公司宣布与苹果公司达成合作⁴⁵，将ChatGPT与苹果iOS、iPadOS和MacOS进一步深度集成，包括苹果操作系统自带的Siri语音助手和各种写作工具等。美国政府机构和情报界的这一番操作可谓“司马昭之心路人皆知”，也标志着“黑客帝国”的大规模监听行动

⁴⁴ <https://www.theverge.com/2024/6/13/24178079/openai-board-paul-nakasone-nsa-safety>

⁴⁵ <https://openai.com/index/openai-and-apple-announce-partnership/>

已经进入“AI时代”。

作为“伏特台风”行动的最主要间接受害人，中国不仅蒙受了“不白之冤”，实际上也是美国最主要的网络攻击战目标。2022年6月22日，以研发先进航空、航天、航海技术著称中国西北工业大学发布公开声明表示遭到境外网络攻击并向公安机关报案。2022年9月国家计算机病毒应急处理中心和360公司组成的联合调查组发布的相关调查报告表明攻击活动源自美国国家安全局的特定入侵行动办公室，报告还提供了攻击事件的总体概貌、技术特征、攻击武器、攻击路径等。2023年7月26日，中国湖北省武汉市应急管理局发布声明表示武汉地震监测中心的部分地震速报数据前端台站采集点网络设备遭到境外组织发动的网络攻击，中方联合调查组对现场提取的木马样本的初步分析表明攻击者也来自美国政府机构支持的黑客组织。

除上述已知案例外，从现有数据分析，在从2023年5月至今的1年时间里，美国政府机构支持背景的黑客组织对中国政府、高校、科研机构、大型企业和关键基础设施的网络攻击活动总数超过4500万次，已被明确遭受攻击的受害单位超过140家，从这些受害单位系统中发现的攻击武器样本指向了美国中央情报局（CIA）、国家安全局（NSA）和联邦调查局（FBI）等部门，这些攻击行动的背后都是“702条款”的授权。

四、结语

“伏特台风”计划再一次向世人展示了美国“金钱政治”的本质，是美国国内不断加剧的“政治斗争”和“利益斗争”以及美国竭力维持的国际霸权的必然产物。美国政客这种为了自身利益向外转移内部矛盾，**严重损害中国利益的行为是全体中国人民不能容忍的**。未来，很可能美国网络安全企业将在美国情报机构的操控下炮制更多虚假“外国政府支持的网络攻击活动”的叙事，不断欺骗美国国会批复更多预算并增加美国纳税人的债务负担。事实上，美国情报机构和军事机构经常以国家安全为由，通过与有关供应商勾结，明目张胆的编制虚假预算，使用来自美国纳税人的政府资金大量购买质次价高的产品实现利益输送。既然美国自诩为国际“法治标杆”、“人权灯塔”，就应该追究这些参与合谋欺诈的政客、官员和私营企业的法律责任。同时，我们也在奉劝美国政客在处理美国国内政治问题时管好自己的事，不要总拿中国当“挡箭牌”，也不要妄想孤立中国和遏制中国的发展。最后，我们也要向全世界警示，美国的“702条款”是美国构建“黑客帝国”的重要法律基础，不仅对美国人民，也是对包括中国在内的全世界所有国家主权安全和公民个人隐私权的严重威胁。我们呼吁各国政府和人民坚决反对和抵制美国利用网络技术优势侵犯他国主权和人民合法利益的恶劣行径。

附件：美国威胁盟公司报告原始版本和最新版本

国家计算机病毒应急处理中心
计算机病毒防治技术国家工程实验室
360 数字安全集团